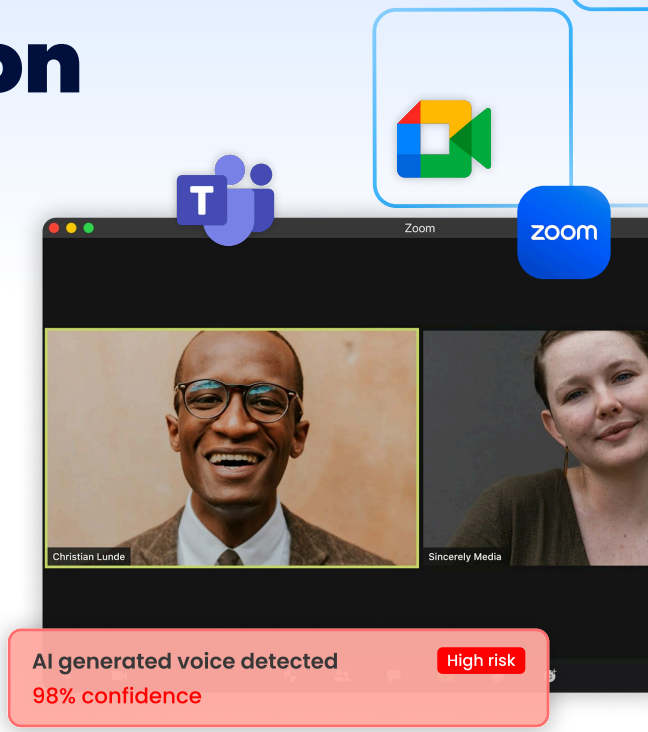
aurigin.ai

# CEO Fraud Protection

## Real-time defense against deepfake impersonation in enterprise communication




## Understanding the threat

Cybercriminals **use AI-generated voices and videos to impersonate executives** across email, phone, and video calls. **Exploiting trust and urgency,** they **deceive employees into transferring funds or disclosing sensitive information.**

*In 2024, an Arup employee in Hong Kong was deceived by a video call featuring deepfake versions of senior executives, leading to unauthorized transfers of over US $25 million.*

Source: Financial Times

## Key challenges

- AI-generated voices and videos now make it **effortless to fake a CEO call** or urgent video meeting
- Traditional cybersecurity tools **can't verify AI generated cloned voices**
- Employees under pressure **act before validating suspicious requests**
- **Lack of awareness** of AI-driven impersonation risks

**5%** **of all frauds are AI voice and/or video generated**

**7x** **annual increase in deepfake fraud**

**$40 billion** **expected cost of deepfake fraud by 2027**

Sources: Deloitte, AFP

## Solution

Aurigin.ai enables organizations to **instantly verify voice authenticity and stop deepfake-based fraud** before it **causes financial or reputational damage.**

- **Instant detection:** Identifies AI-generated voices in real-time
- **Continuous protection:** Monitors, alerts, and logs incidents for compliance and audit readiness
- **Seamless Integration:** Works across Teams, Meet, Zoom, and enterprise communication systems
- **Flexible deployment:** Cloud, on-prem, or isolated environments for full data privacy

**98% accuracy** | **40+ languages** | **<50ms latency**

EY swisscom 1291 GROUP venturelab VERIFYLABS.AI TRUSTED INFORMATION ALLIANCE

Aurigin.ai AG

info@aurigin.ai

www.aurigin.ai